Seid Alimostafa Sanglakhi

Hackers and the Internet

Helsinki Metropolia University of Applied Sciences

Bachelor of Engineering

Information Technology

Thesis

17 June 2013

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Seid Alimostafa Sanglakhi Hackers and the Internet 36 sivua 17 Kesäkuu 2013
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Sulautetut järjestelmät
Ohjaaja(t)	Pasi Ranne, Tuntiopettaja

Opinnäytetyön tavoitteena oli tutkia Internetin ja hakerointtia uusia nykyaikana ja tulevaisuudessa yleistyviä tekniikoita ja verkko hyökkäyksiä ja verkkopuolustuksen tekniikoita. Myös selvittää miltä tulevaisuudessa tietoturva näyttää verkko hyökkäyksien ja verkko puolustuksen näkökulmalta.

Tehtävänä olisi selvittää, millä tekniikoilla hakkerit hyökkäävät ja miten voidaan puolustaa itseämme hyökkäyksestä. Lisäksi työssä käsitellään internetin turvallisuutta laajasti sillä että se johtaa meitä siihen suuntaan jotta opimme tärkeitä asioita. Miten nykyaika muutokset vaikuttavat internetin yleiseen tietoturvaan, lisäksi tietokoneen käyttäjien rooli muutoksissa. Koska ihmiset yleensä eivät huomaa paljon hakerointti tuottaa harmia maailman talouteen.

Lopputyön aiheen tarkoituksena oli valmistella hyviä viitteitä opiskelijoille myös muille halukkaille jotka haluavat oppia tästä uudesta teknologiasta. Nykyään on tärkeää että jokaisella on hyvää tietoa tästä tietokoneen ja internetin turvallisuudesta koska yritykset ja organisaatiot käyttävät päivittäin työnteossa ja niiden varten pitäisi oppia miten he tulevat toimeen sen uhatukseen kanssa.

Avainsanat	hacking, hackers, internet, security

Author(s) Title Number of Pages Date	Seid Alimostafa Sanglakhi Hackers and the Internet 36 pages 17 June 2013
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Embedded Systems
Instructor(s)	Pasi Ranne, Lecturer

The purpose of this project was to study hacking and hackers. It focused on learning the best ways to make the internet secure. The thesis investigates hacking and hackers as threats to internet security. The scope of analysis encompasses various fields of technology. Consequently, the conclusive observations provide a good understanding and information on protecting valuable internet resources from criminal and malicious users that harm personal and business information security.

People often do not realize how much computer crime is costing the global economy.If the basics are understood, fewer people should be affected which would cost the economy less.

The project was aimed at providing useful information about hacking and the internet for students. This would also include ordinary people who want to learn more and be better informed about this rapidly growing computer technology. Nowadays it is very important to have a good knowledge about computer and internet security because organizations and companies and also ordinary people are using the internet for daily activities. Reading this thesis helps people become familiar with these threats.

Keywords	hacking, hackers, internet, security

Contents

TIIVISTELMÄ

ABSTRACT

1 Introduction

2 Types of Hackers

2.1 Sumurais
2.2 Crackers
2.3 Wackers

3 Easiest Ways to Hack

3.1 Viruses
3.2 Sending Secret Messages
3.3 Serial Number Prediction Attack (Attack on IP)
3.4 Denial of Service (DOS)
3.5 Password Cracking
3.6 Packet Sequence Attack
3.7 Defending against Hacker Attacks

4 Forgery

4.1 E-mail Forgery
4.2 Web Forgery
4.2.1 Cross Site Scripting and Stealing Cookies
4.2.2 Cross Site Request Forgery (CSRF)
4.3 Discovering Forgery

5 Types of Network Scanning

5.1 Network Mapping
5.2 Port Scanning
5.3 Service and Version Detection
5.4 Dos Detection

6 Social Engineering

6.1 Gaining Trust
6.2 Protection

7 Introduction to Fundamental Concepts of the Internet

7.1 Internet Infrastructure
7.2 Hierarchy of Computer Networks
7.3 Internet Applications
7.4 WWE (Word Wide Web)
7.5 FTP (File Transfer Protocol)
7.6 Email
7.7 TelNet
7.8 Motor Engine
7.9 Websites
7.10 Webpages
7.11 WEB Browser

8 Basic Information about Security

8.1 Active Content Monitoring
8.2 Access Control
8.3 Trojan Horses
8.4 Worms
8.5 Spy Ware
8.6 Spam
8.7 Cookies
8.8 Fire Walls
8.9 Anti Virus Software
8.10 Encryption
8.11 Symmetric and Public Keys

9 Conclusion

References

Acronyms

SSL	Secure Sockets Layer
SMPT	Simple Mail Transfer Protocol
ASCII	American Standard Code for Information Interchange
DNS	Domain Name System
TCP	Transmission Control Protocol
IP	Internet Protocol
POP	Point of Presence
NAP	Network Access Points
ISP	Internet Service Provider
WWE	Word Wide Web
FTP	File Transfer Protocol
Email	Electronic Mail
LAN	Local Area Network
WAN	Wide Area Network
WLAN	Wireless Local Area Network
Sumurai	White Hat Hackers
Cracker	Black Hat Hackers
Wacker	Wannabe Hacker or Script Kiddies

1 Introduction

Studies show that there has been a rapid growth of knowledge and technology over the past centuries. During the twenty-first century, information handling has become more important, as the technology of collecting, processing and distributing information has become important.

In addition to these innovations, including large telecommunication networks, the development of the growing computer industry and satellites is important although the computer industry compared to other technologies such as genomics and robotics seems old. All in all computers can do a lot in a short period of time, which has led to a growing and effective application in various branches of sciences.

The integration of computers and the field of communication networks has been named computer science. Many networks have benefited users even if there is a possiblity that hackers are seeking to achieve their own goals.

This is not to say that new technologies such as the internet and networks are intrinsically bad, as many people would have people to believe. They are simply a means for human beings to express themselves and share common interests. Hacking is also a greatly misrepresented activity by the wider media such as movies, TV and magazines. Generally speaking many computer enthusiasts become system administrators, security consultants or website managers.

As a result, the goal of this thesis is to give a brief overview of hacking and the internet without going into too much detail of any particular technique. So ways of making the internet and computer systems secure, so that noboday can misuse them, are focused on. Firstly hackers and hacker types are discussed, and then their ways of creating viruses, secret messages and so on.

A brief introduction is given in chapter 1. Subsequently, the topic is further discussed in chapters 4 – 7. Finally, chapter 8 deals with security and the issues which shuold be kept in mind when protecting people's privacy online and avoiding any kind of danger or putting privacy at risk on the internet.

Studies show that there has been a rapid growth of knowledge and technology over the past centuries. During the twenty-first century, information handling has become more important, as the technology of collecting, processing and distributing information has become important.

In addition to these innovations, including large telecommunication networks, the development of the growing computer industry and satellites is important although the computer industry compared to other technologies such as genomics and robotics seems old. All in all computers can do a lot in a short period of time, which has led to a growing and effective application in various branches of sciences.

2 Types of Hackers

Firstly, it is best to define who is a hacker. Hackers are smart people who do not have interest in a permanent job at the start and usually they have other intentions than money. The first principle of this group is free information for all and they think that it is their right to use the data and programs of other people. First of all, it is necessary to understand the real definition of a hacker or hacking. It is very important to know what a hacker is not. [1]

First of all, a hacker is definitely not a criminal. A hacker is not a person who is breaking the law and releasing viruses and so on. A hacker is also not teenager sitting in a dark room in some corner and eating pizza the whole day. [2]

A hacker is also not somebody who is good at acts and breaking wood and creating very good furniture. Surprisingly, a hacker is also not always a computer wizard and also not somebody who can break and crack passwords to all websites and to all applications and to all software. [2]

Then who is exactly a hacker? The real definition of a hacker is actually a person who has some very interesting qualities or characteristics. First of all, a hacker is somebody who likes to think out of the box, he is somebody who always likes to achieve things that normally are not achievable and things that most people do not even think about. [2]

A hacker is always somebody who wants to discover new features and new characteristics, new tricks and also make things work in a manner that most people never think about or imagine. [3]

A hacker is a person who is highly creative and highly innovative and can actually think and achieve things. These characteristics define what a hacker really is. The most

famous scientists and inventors and creative people fit into the definition of a hacker. Hackers can be put into three catefories which are discussed below [3].

2.1 Sumurais

Sumurais are hackers whose only interest is to use a victim's computer, but they do not cause damage to the victims' computers. The first principle of this group is freedom of information for all and their intention is to show a computer's weaknesses and lack of protection. They help the police or other legitimate financial institutions to protect companies' inside information or secret information. [4]

2.2 Crackers

Crackers are hackers and their goal is to steal information and vandalism on the computer. The intent is to hide in a corner and cause damages. A cracker has the same experience and the same knowledge as a sumurai. The only difference between a cracker and sumurai is the fact that a sumurai is a good guy and a cracker is a bad guy. In fact, the most dangerous hacker is a cracker who uses and causes damage and sabotages to the victim's information. A sumurai is somebody who utilizes the information in a positive sense and helps the police agencies but a cracker is the opposite. [5]

2.3 Wackers

Another type of a hacker is a wacker, who aims to use private information from a victim's computer. This type of hacker does not have a lot of information about a

computer system and programming so they are seeking around the internet and seeking free tools and using them. In fact they are dangreous because they do not know much about what they are doing. They do whatever they do just for an entertaining moment.

3 Easiest Ways to Hack

People often do not realise how much computer crime is costing the global economy. Accroding to a new study by Symantic, hacking costs the gloabl economy 114 bilion dollars each year. Thus if the time is counted that is lost by companies trying to recover from an attack, another 274 bilion dollars can be added to that number [6], as figure 2 suggests.

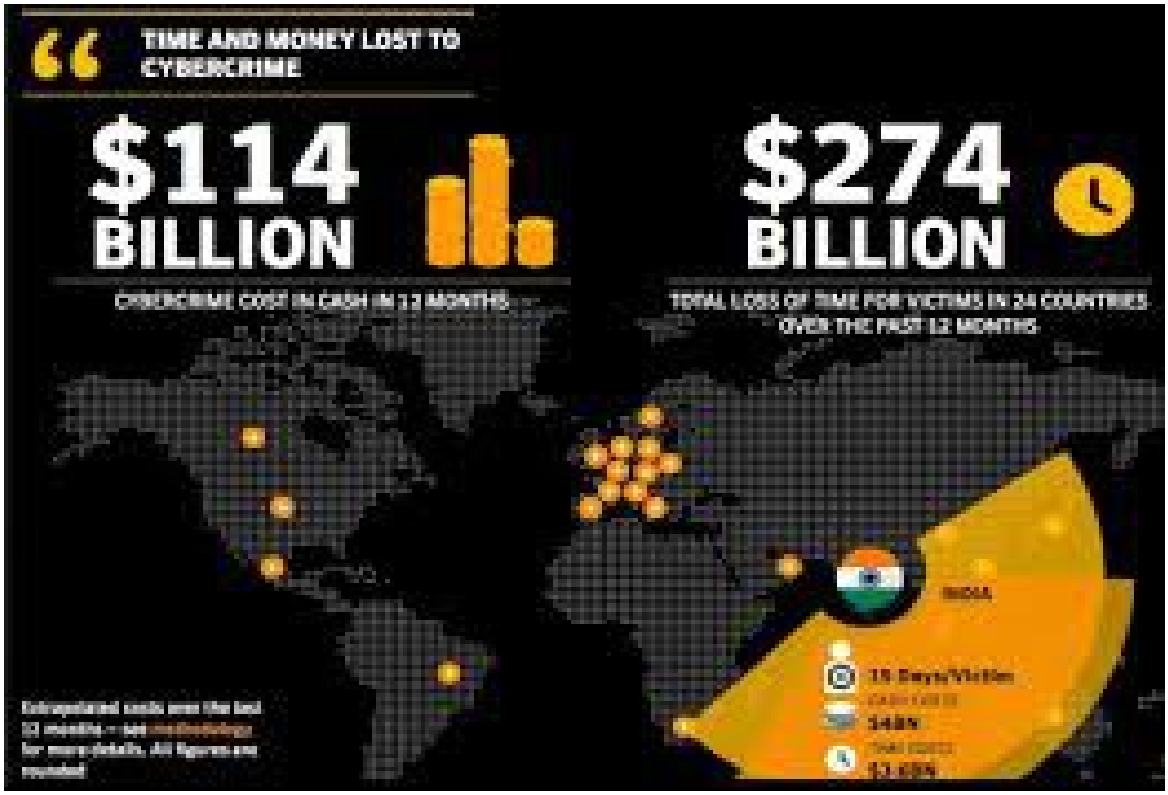

Figure 1. Time and money lost to CyberCrime [7]

If why it is happening and how to react are figured out, fewer feople should be affected, and this would cost the economy less. There are many methods available to hackers attacking a system. A brief overview is provided of some of the more common techniques.First of all, it should be known that hacking is a two-step process: gathering information and lauching an attack.

3.1 Viruses

In summary, viruses are programs that work in the short run and reproduce without notice on a host computer and other computers. Under certain circumstances, these cause destruction on the computer system.

This could include the destruction or loss of critical information. All information is available on the victim computer. For this purpose, viruses have been reproduced in the system, and they use different tools such as diskettes and CD or mail to infect other users within a short time.

A virus can infect all the computers in a network before its implementation is identified and it is possible to try to prevent its intentions and the destructions it might cause. First of all, hackers put a program into user requested information and thus will influence the user's computer.

3.2 Sending Secret Messages

Sometimes hackers want to share some issues to individuals or personal references with a person and yet remain anonymous. For this reason in order to be anonymous, they use software called Ghost mail which is available on various web sites and it is imposibble to be tracked and identified. Search engines such as Google or Yahoo can be used to find the software.

3.3 Serial Number Prediction Attacks (Attack on IP)

In order to be identified on the Internet, every computer has a unique address in the virtual world. These virtual addresses are a series of numbers separated by dots, some of which may never be repeated.

It generally follows this pattern: xxxx.xxxx.xxxx.xxxx. For example, 126.254.63.69 is the IP address of computer A. This is a unique address of computer A. In this attack, the hacker starts its work in two steps.

In the first step, a hacker usually tries to obtain the IP address of the server. Because the hacker knows that the other computers on the network have the IP addresses which are part of the address of a shared server, so he tries to simulate the number of an IP address. This allows him to pass a router and gain exposure which gives to the hacker access to the local user system. For example, if the system has the address 192.168.0.15, a hacker knows that a maximum of 256 computers can be connected to the network and they may be third class. A hacker tries all numbers in the range of addresses so it makes easier to guess the last byte. The last IP addresses of computers connected to a network show the two bits worth 128.

Secondly, once a hacker guesses the range of addresses in the network, he can generate packets with the correct serial numbers and IP addresses, and business exchanges to influence others.

3.4 Denial of Service (DOS)

As for Denial of Service a hacker basically tries to sabotage a service running on a port on the targeted system. The purpose of this attack is to disable the service and prevent people from accessing that service such as a web server.

3.5 Password Cracking

The purpose of a password cracking attack is to decrypt or otherwise disable password protection. Most password crackers are brute force engines that try a word after word at a very fast speed.

3.6 Packet Sequence Attacks

As for Packet Sequence Attacks, hackers try to guess the random sequence of numbers of the TCP packet, and by doing this, they can insert their own packet into the connection stream.

3.7 Defending against Hacker Attacks

The simplest and most efficient way to protect against a hacker's attacks on serial numbers is to make sure the security of each router, firewall and system has been considered.

4 Forgery

It is assumed in services that the IP address of the host is a valid address and therefore it can be relied on it. However, a hacker can forge its IP address to a valid host and acts as valid user.

The following gives an example of how a hacker can forge the valid user computer:

1. A hacker can forge the IP address of a host according to a user's address.
2. A hacker then makes an address for the server which is the direct path between the server and the address of the hacker.
3. A hacker uses the source address of the user request and sends it to the server.
4. When the request comes directly from the user to the server, it is accepted and a response is sent.
5. A valid user using the hacker host sends the packet to the source.

4.1 E-mail Forgery

On the internet, it is very easy to forge an email message and often senders can not be trusted without security tools like digital signatures. For example, this can be imagined in a short online exchange between hosts. The name is an exchange, so the protocol for the exchange is based on ASCII codes. Telnet can simply be connected to a port of SMPT. The receiver trusts the sender's profile and the hacker can easily with different addresses attached forge the address.

4.2 Web Forgery

Web forgery is another method of hackers to do attacks. In this method, they make a copy of the entire web which has all the trapping of the original website. The difference is that it is completely controlled by hackers. As a result, all transactions between users' browsers and the web are seen by the hackers. A hacker goes further and right now attacks secure sites and develops websites based on SSL.

Currently SSL uses the DNS name in its certificates. For secure and reliable exchange of business, the data found in the server browser sends the private key. With regard to forgering the address bar, SSL has no problem. However, since all addresses on web pages do not use SSL, it possible to forge the addresses. A session can be stolen from a nromal user. When we buy something from webshop, this may be happen.

4.2.1 Cross Site Scripting and Stealing Cookies

Some sites store user credentials in cookies. Thus, by using or stealing cookies a hcker can pretend to be some one else. By stealing cookies, a session can be stolen from a normal user. This could happen, for example, when a user is using a web-shop. After stealing session-ids, an attacker could order items from a web-shop using another person's account.

4.2.2 Cross Site Request Forgery (CSRF)

Cross Site Request Forgery will be happen, when a user visits a guest book and decides to visit some other site as well. The other site might be controlled by an attacker that has injected a special attack code in the page.

5 Types of Network Scanning

Network scanning is the process of discovering active hosts on the network and information about hosts, such as operating system, active ports, services and application. Here are the basic four techniques:

Network Mapping: Sending a message to a host that will generate a response if the host is active.

Port Scanning: Sending a message to a specified port to determine if it is active or not.

Service and Version Detection: Sending a specially crafted message to an active port to generate responses that will indicate the type and version of the service running.

Dos Detection: Sending specially crafted messages to an active host to generate certain responses that will indicate the type of the operating system running on the host.

Also, there are more than four techniques but these are not mentioned because they are out of the scope of this thesis. [8]
Furthermore, flowing can be expected from a network scan, as table 1 suggests.

Table 1. Network scanning output

Host 192.168.99.1	
Open ports include	
	135 / TCP open msrp
	139 / TCP open netbios-ssn
	445 / TCP open microsoft-ds
	3389 / TCP open ms-term-serv
The operating system is windows 7 SP1	

Details about a security scanner called Zenmap are given below (see figure 2). Zenmap is a multi-platform (Linux, Windows, Mac OS) and free and open source application. This is very easy to use and it can also provide many good things for both users such as beginners and also experienced users.

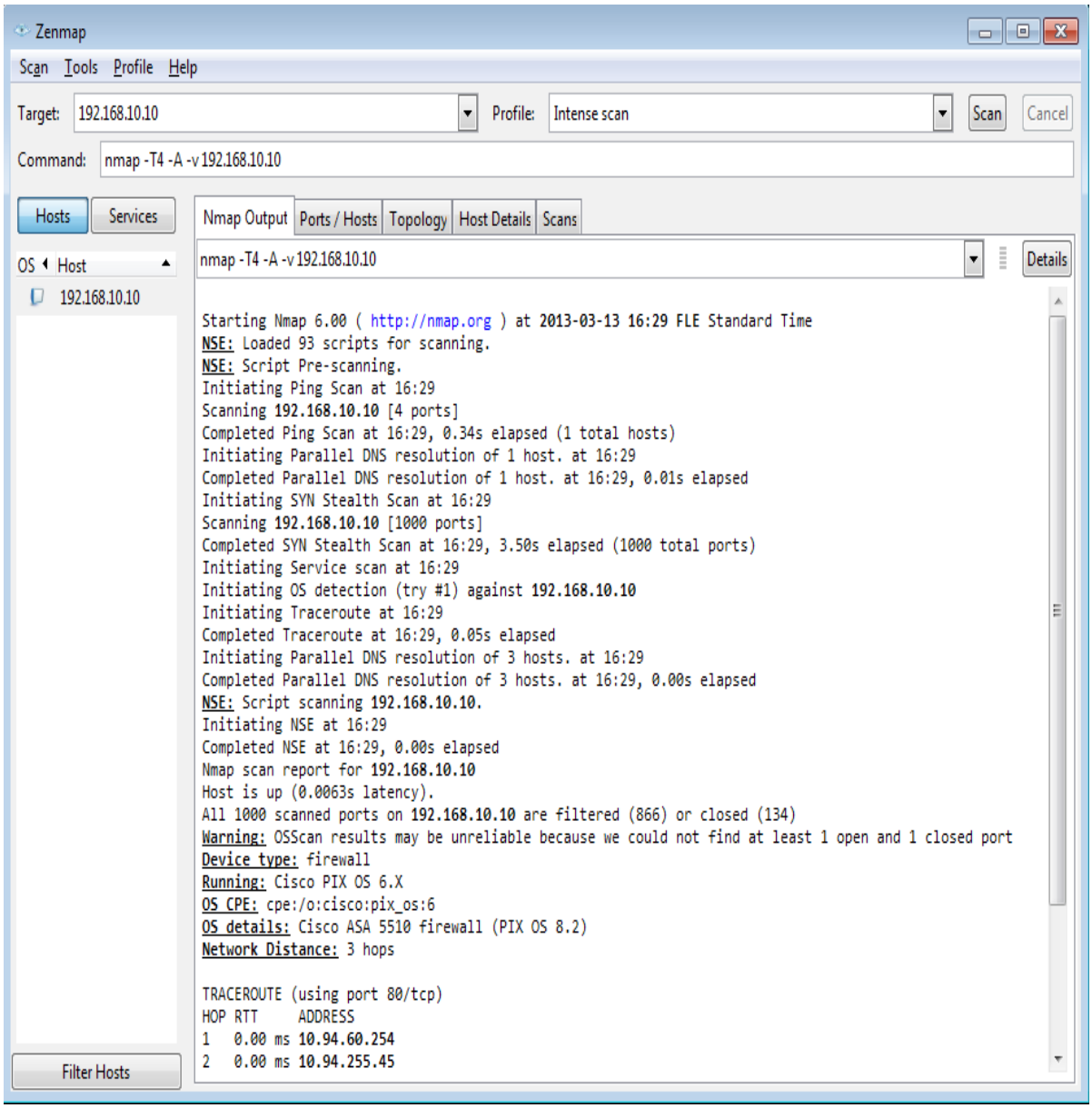

Figure 2. Zenmap Security Scanner GUI (Snipping Tool)

First of all, Zenmap is a graphical user interface. It is very easy to use and the first question is how this can be used or how it works? It is necessary to put an IP address.

The target field and click the Scan button. If should be typed a range of IP addresses is scanned, then the beginning IP address should be typed followed by (no spaces), a dash (-) and the end of the last IP address. For example, if somebody wanted to scan 192.168.1.100 to 192.168.1.299, then It would be necessary to type *192.168.1.100-299*. When one scan is finished, all the information in Nmap output can be seen. Then the port/host and topology and host details can be checked in a separate view. Another thing that is very good is that, another IP address can be scaned as soon as the first scan has finished, so it is possible to have both of the scans' information at the same time. As figure 3 shows.

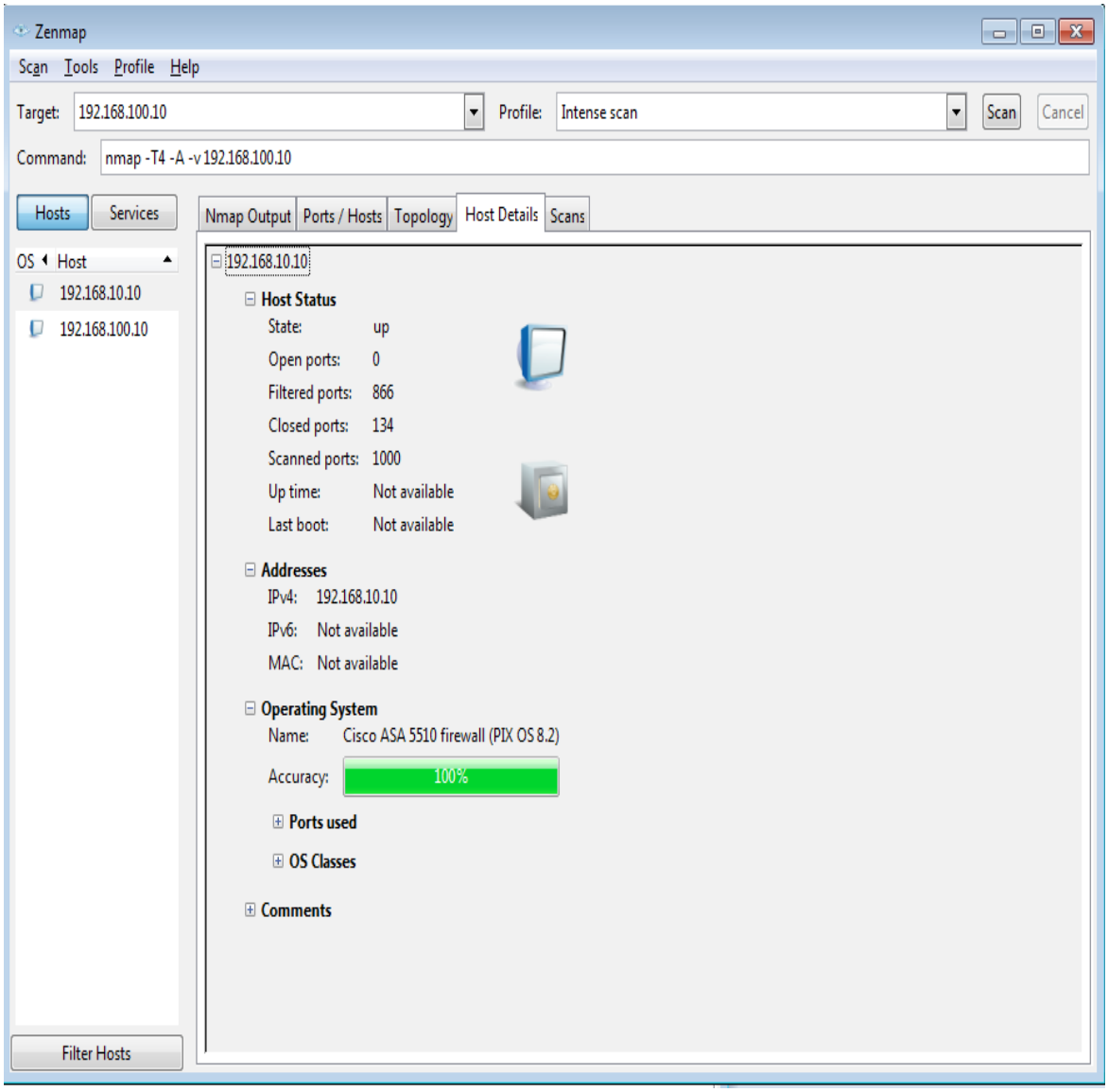

Figure 3. Zenmap Security Scanner GUI (Host Detail)(Snipping Tool)

6 Social Engineering

Social engineering is the art of gaining access to information, system or data by exploiting the psychology of human beings rather than using technical hacking techniques. For example, instead of finding some software to obtain the information, social engineering refers to using a human being manner to do it.

Frankly a student or an employee can be called and the caller can act as a school IT support person or police or somebody else and ask the student to give his password or system password or some other information. The main issue is to gain the trust of one or more people. [9]

6.1 Gaining Trust

Social engineering does not require a significant amount of technical skills to be successful at gaining trust or confidential information, and because of this, this is very dangerous.

In summary, social engineers are looking for information to lead to taking an advantage of others.

There is a list below of some items that social engineers try to gain:

-Password

-Account numbers

-Keys

-Any personal information

-Phone lists

-Detais of the computer system

-The name of someone with access privilege

-Information about the server, network and URL and the internet

There are a few basic psychological tactics that social engineers use to gain trust and get what they want.

1. Acting confident
2. Offering free gifts or favors
3. Using humor
4. Giving some (logical) reason

Network scanning is the process of discovering active hosts on the network and information about hosts, such as operating system, active ports, services and application.

6.2 Protection

It is necessary to keep in mind that if somebody asks for credentials, they are not trustworthy, because the bank or some other security companies or legitimate financial institutions will never ask for the credentials through email or phone. As a result, it wise to trust anyone who is asking for personal information or credentials or never to show or provide personal information to anyone.

7 Introduction to Fundamental Concepts of Internet

7.1 Internet Infrastructure

The Internet is a computer network (large, small). A computer network is a group of computers that communicate with each other. These networks are using computers connected to each other and an entity called "the Internet" has been created.

The Internet began its initial operations in 1969 and started with four host computers. After host developing, an incredible number of host computers exist on the network nowadays and there are more than 10 million users. The Internet does not belong to any particular organization or institution in the world.

7.2 Hierarchy of Computer Networks

Every computer that is connected to the network is considered as part of the network. For example a home phone connected to an Internet service provider can be used and which enables using the Internet. In this case the computer will belong to a large network. The Internet is composed of numerous networks (a network of other networks), as figure 4 shows.

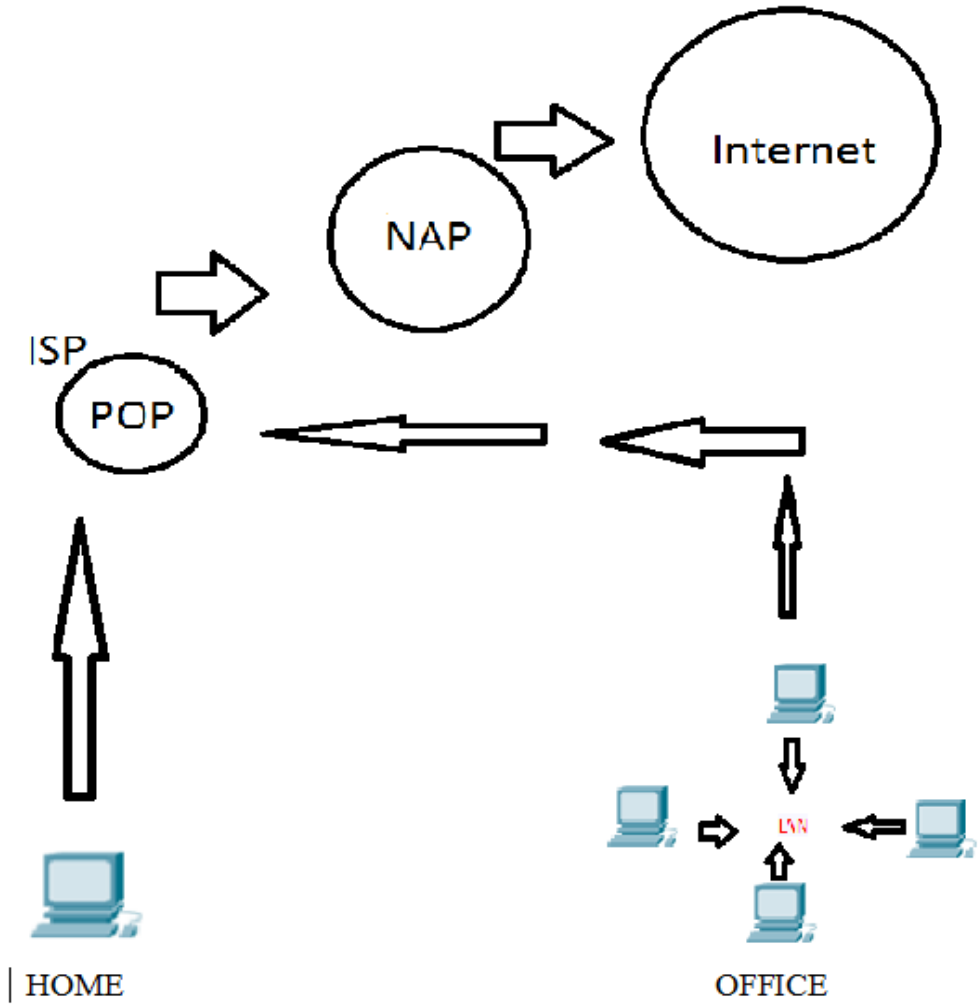

Figure 4. Numerous Networks

Most large communications companies have dedicated backbone to connect different areas.

7.3 Internet Applications

- The major uses of the Internet can be named as follows:
- E-mail
- Chat

- Conference newsgroups
- Conference newsgroups
- Reading the news
- Office Internet in libraries
- Buying needed goods
- Opportunity to study
- Watching TV and listening to radio
- Obtaining information regarding the different
- Fun and games

7.4 WWW (World Wide Web)

The World Wide Web is commonly known as the web. What the general public knows about the web, is only one of the most popular internet services in the name of the web service. The web is the latest internet tool which is growing very rapidly. A web tool is based on hypertext that allows finding information through search based on keywords. The web is one of the services that runs on the Internet and it collects text documents and other resources. To see a webpage on the World Wide Web, the URL of the page should be typed into a web browser.

7.5 FTP (File Transfer Protocol)

A tool called file transfer protocol (FTP). FTP allows the user to move a file from one location to another on the Internet. FTP is often secured with SSL/TLS (FTP). SSH File Transfer Protocol (SFTP) is also used but it is technologically different. FTP uses the Internet's TCP/IP protocols to enable data transfer, and it is mostly used to download files from a server using the Internet or to upload a file or movies to a server.

7.6 Email

Email comes from the words ”electronic mail”. It is an acronym of electronic mail. Each individual can send message to each other around the world. This service acts as an e-mail electronically and will perform on the web. Nowadays there are very popular free email servises such as Gmail, Hotmail, Yahoo, Mail and GMX Mail.

7.7 TelNet

TelNet is a term that refers to remote logging and it is a tool that makes it possible to access and control a computer on the Internet. With these capabilities, it is possible to access another computer. This service is usually used for searching databases of public information, archives or library resources. For example, there is a weather reporting system in the United State of America and anyone can enter this system and study the weather in his or her area.

7.8 Motor Engine

A search engine uses a program-specific data that can be entered by the user to search huge databases and it shows the results to the user. Nowadays people use search engines such as Google, Yahoo, Bing and others to look for information on the world wide web. Also some other focused search engines exist such as Academic Search Encines, Meta Search Engines, Media Search Engines and Social Search Engines. These are some examples of those: Google Scholar, iSEEK, OJOSE, Scircus , DMOZ, Whonu, Info.com, Pixsy, Blinkx, iSearch and so on.

7.9 Websites

Websites are database applications that run on a Web server. Users can also make use of the information they provide. A web site is a simple site and it has unique web domain name and it is hosted on at least one web server. Usually a website contains a home page, which is the first document users see. The site also may contain some additional documents and files. Each site is usually managed by a company, an organization, or an individual.

7.10 Webpages

When somebody tries to obtain information from a particular webpage, the main server information on that particular site is displayed on the computer screen. Every web page is identified by a unique URL. This is a web document that is suitable for the world wide web and can be accessed through a web browser and it can be seen on a monitor or mobile device, and this information is usually in HTML or XHTML format.

7.11 Web Browser

To do any action, using a special computer software is required. This particular software is called a web browser. A web browser enables computer users to access web pages. Browsers translate HTML (Hypertext Mark Up Language) code that allows us seeing images, video and listening to music on websites. Nowadays there are many types of browsers such as Mozilla Fire Fox, Netscape Nacigatros and Microsoft Internet Explorer.

8 Basic Information about Security

To have a good and secure system, it should be understood who might be able to access the systems or who might be the enemy. Otherwise, the systems are not protected from cyber crimes.

Firstly, the enemies should be known. If there has been good knowledge about computer systems then, it is easier to undrestand the nature of the threat. Good undrestanding means that if there has been an attack somehow or by someone, then there should be some footprint all over the computer when scanning is implemented. Thus, the next step is to recognize who attacked and how it happened which should be possible by finding these signs or clues.

It is very important to keep others away from a computer that needs to be protected because physical access to a computer means that security is at risk, so credentials information should be put in a safe palce so that nobody has access to it.

Another thing is access to LAN or Server. It is very important that a good password is chosen so that nobody has access to it. In large companies physical security is important and no one expect personal staff should have access to a password. Also access to LAN should be impossible to anyone but authorized personnel.

People should not use or choose an easily guessed password for local area network connections. A password with a part of our name or family or relative's name should not be used. Also using an acronym or mnemonic will not be safe. So how should password be chosen? The first thing is to choose a name and a few numbers and some other marks that would be a good and safe password. Also what was said about social engineering is importan, namely that a password should not be given to anyone under any cicumstances.

8.1 Active Content Monitoring

Active content can make web browsing more enjoyable by providing toolbars, stock tickers, video, animated content, and many more interesting things.
Thus, why is it needed? To answer this question, some basic things have to be known, which are saving time and money and providing a content safe network. [10]

8.2 Access Control

Access Control refers to security features that control who can access all kinds of documents or resources in an operating system. Access Contorl describes the security model for controlling access to Windows objects, such as files and the administrating function such as setting the system time or installing a program on the computer admin that have access to all computer programs.

8.3 Trojan Horses

A Trojan horse, or Trojan, is a type of malware which appears to perform a desirable function but instead facilitates unauthorized access to the users' computer system [11]. Trojans do not attempt to inject themselves into other files like a computer virus. Trojan horses may steal information, or harm their host computer systems [11]. Trojan horses present themselves as useful and harmless programs or useful things in order to persuate victims or users to install them on their computer. After they have been installed, they begin their operation.

In order to protect oneself from Trojan horses, the easiest way is to not open e-mail or download any attachments from unkown senders. If the sender should not be known then any (.exe) file should not be opened unless the sender can be trusted

completely. Simply these messages should be deleted and this will take care of the situation. Antivirus software should be installed that scans every file that has been downloaded.

If the computer has been infected with a torjan, interent connection should be disconnected and the files in question should be removed with an antivirus program or by installing the operating system again.

8.4 Worms

Computer worms are malicious software applications that are designed to spread via computer networks. A computer user typically installs worms by opening an unsolicited email attachment or message that contains executable scripts such as (.exe) [12]. They may also open a TCP port to create network security holes for other applications to take advantage.

8.5 Spy Ware

Spy ware is any software that secretly gathers computer data or user information through the user's Internet connection without his or her knowledge. Usually the intention behind it is advertising purposes. Spyware is similiar to a Trojan horse [13].

8.6 Spam

Spam is most often considered to be electronic junk mail or junk newsgroup postings. Real spam is generally email advertising some product sent to a mailing list. The purpose of spam is to advertise products and gather more and more people to see and show what they have to bring to the society.

8.7 Cookies

The purpose of cookies is that a web server sends a message to a Web browser. The browser stores the message in a text file. The message is then sent back to the server each time the browser requests a page from the server. The main issue is to go to a webpage in the fastest time that is possible [14]. An example is given below because a picture tells more than a thousand words.

Figure 5. Cookies on the BBC weBsite (Snipping Tool) [16]

8.8 Fire Wall

The purpose of a network firewall is to provide a safe place around the network which will protect a computer on the network from various computer threats.
The types of threats a firewall can protect against include:

- Unauthorized access to network resources
- Masquerading
- Denial of service

8.9 Anti Virus Software

The best tool against hackers and any viruses is Anti Virus software which nowadays is very much part of IT security. There are also more things that should be kept in mind such as back ups and password checking.

If systems are infected by viruses in a large company, this might cost a few thousand euros to correct. There are many anti-virus packages on the market and a suitable one it can be chosen from them. Anti virus is easy to install and here is a list of a few good anti virus:

- F-Secure Anti Virus
- AVG Anti Virus
- Norton Anti Virus
- Bitdefender Anti Virus plus

System security should be taken seriously. Finally, it is necessary to learn to assess security for oneself and use the same attitudes and tools that black hat hackers use.

8.10 Encryption

A variety of methods should be found about information security on the internet. The question is how data or information can be kept safe. It is very simple, data should be put on removable storage media like portable flash memory drives or an external hard drive. Nowadays there are very popular forms of security which all rely on encryption. With an apropriate encryption method, only the person with the key can decode it. Whenever there is talk about computer enctyption systems, one of these two categories are generally reffered to:

- Symmetric-key encryption
- public-key encryption

8.11 Symmetric and Public Keys

In symmetric and public Keys methods each computer has a secret key that it can use to encrypt a packet before sending information to another computer over the network. In this way, the key should be known. For example if information is sent to another computer, the key should be installed on both computers. Otherwise, it does not work.

With this method, there should be two keys at once, namely the private key and public key. The private key is known only on the sender computer and the public key is given to any computer that wants to communicate securely with it. File encryption is the best option if it is considered to keep foreign spies, or annoying roommates out of files. Figure 5 presents six of the most popular encryption tools to lock down files.

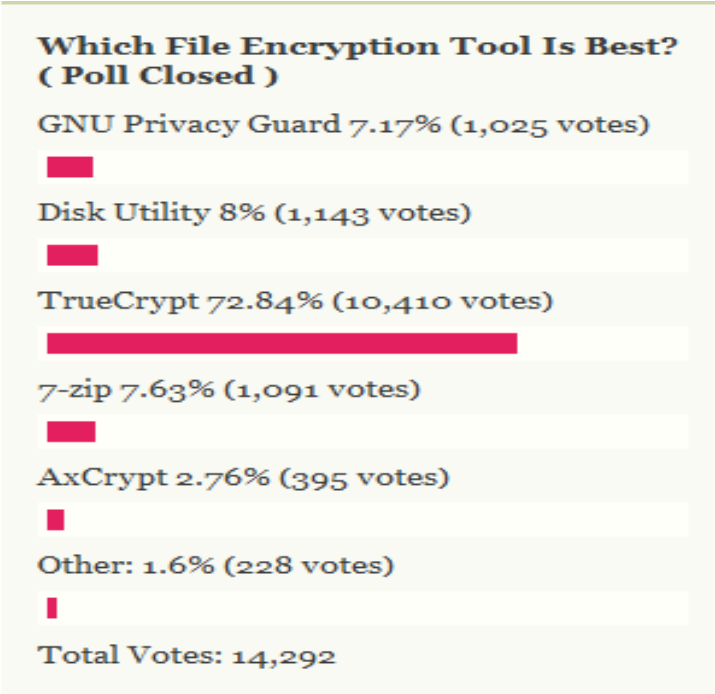

Figure 6. Best File Encryption tools (Snipping Tool) [17]

9 Conclusion

The main idea of the internet to me is the possibility it gives to communicate in a cheap and creative way. This ability may be web design, chat rooms and email and so on, because no other media in the history has provided such a level playing field, where an induvidual could compete with the big corporation to have their voice heard online.

Nowadays life can be a little bit of a mine field especially when it comes to avoiding hacker attacks, so most people know the basic advice given such as useing a fully up-dated anti-virus product and avoiding surfing to darker parts of the web. These are all important but there are also a few additional things that can be done to secure online presence and keep hackers away.

The motivation behind all viruses and malware hase changed over the years. It should be noticed that earlier they were not developing for specific purpose. However, now they are developed for specific reasons or purposes such as the Stuxnet virus which destroyed several centrifuges used for Iran’s nuclear enrichment program and caused damage to Iran's nuclear infrastructure.[2]

In addition, there are more viruses such as flames which in contrast to Stuxnet, the newly identified virus, are designed not to do damage but to collect information secretly from a wide variety of sources. [2]

Cyber threat is one of the most serious economic and national security challenges that people face today. As a result, knowledge about cyber threats should be improved and cyber threats should be reduced. This does not mean that the threat does not exit, but all internet users should protect their privacy so they should educate and inform them-selves of the more serious risks on the internet.

References

1. Hacking and hackers [online]. November 1, 2012.
URL: http://www.thocp.net/reference/hacking/hacking.htm#general.
Accessed November 1, 2012.

2. Internet security for IT pro [online]. eSeccurity Planet. November 1, 2012.
URL: http://www.esecurityplanet.com/hackers. Accessed November 1, 2012.

3. Sean Michael Kerner. How hackers can benifits IT security [online].
October 18, 2011. URL: http://www.esecurityplanet.com/hackers/how-hackers-can-benefit-it-security-.html. Accessed November 22, 2012.

4. Samurai (hacking) [online]. November 1, 2012.
URL: http://www.fact-index.com/s/sa/samurai__hacking_.html.
Accessed November 1, 2012.

5. Cracker [online]. November 1, 2012
URL: http://www.fact-index.com/s/se/security_cracking.html.
Accessed November 1, 2012.

6. Cyber Crime [online]. February 10, 2013.
URL: http://www.pcmag.com/article2/0,2817,2392570,00.asp.
Accessed February 10, 2013.

7. Copied from Internet[online]. February 10, 2013.
URL: http://www.techinasia.com/cyber-crime-asia/. Accessed February 10, 2013.

8. Network Security Assessment[online]. February 5, 2013.
URL: http://www.professionalsecuritytesters.org/Documents/networkassessment/nsa.pdf. Accessed February 5, 2013.

9. Social engineering [online]. February 1, 2013.
URL: http://en.wikipedia.org/wiki/Social_engineering_(security).
Accessed February 1, 2013.

10. Lande Simon. Three reasons content monitoring keeps your site launch on [online]. November 4, 2011.
URL: http://blog.activestandards.com/three-reasons-content-monitoring-keeps-your-site-launch-on-target/#.html. Accessed February 10, 2013.

11. Trojan Horse[online]. February 5, 2013.
URL: http://en.wikipedia.org/wiki/Trojan_horse_%28computing%29/#.
Accessed February 5, 2013.

12. Computer worm[online]. February 5, 2013.
URL: http://en.wikipedia.org/wiki/Computer_worm/#.html.
Accessed February 5, 2013.

13. Spy ware [online]. February 5, 2013.
URL: http://en.wikipedia.org/wiki/Spyware.html.
Accessed February 5, 2013.

14. Cookie[online]. February 5, 2013.
URL: http://en.wikipedia.org/wiki/HTTP_cookie/#.Html.
Accessed February 5, 2013.

15. Computer System and Network Security.
CRC Press, Inc; 1996.

16. Cookie[online]. February 5, 2013.
URL: http://www.bbc.co.uk/persian/.Html.
Accessed February 5, 2013.

17. Five-best-file-encryption-tools [online]. February 5, 2013.
URL: http://lifehacker.com/5677725/five-best-file-encryption-tools.Html.
Accessed February 5, 2013.